ABSTRACT

In a method for operating a conditional access system for broadcast applications, the conditional access system comprising a number of subscribers and each subscriber having a terminal including a conditional access module and a secure device for storing entitlements, a source signal is encrypted using a first key (C_W). The encrypted source signal is broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, the ECM's comprising the first keys (C_W) encrypted using a service key (P_T). Entitlement management messages (EMM's) are sent to the secure devices providing the service key (P_T) required to decrypt encrypted first keys (C_W). A cracked secure device which is used in an unauthorised manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate. To this end search EMM's are sent to at least a part of the terminals, the search EMM's providing at least the service key (P_T) and a dummy key (P_{D1} or P_{D2}). At least the search EMM's comprise identifiers identifying the keys (P_T and P_{D1} or P_{D2}), wherein first search EMM's with the keys (P_T and P_{D1}) are sent to a first part of the terminals and second search EMM's with the keys (P_T and P_{D2}) are sent to a second part of the terminals An ECM identifying the service key (P_T) to be used to decrypt the encrypted first key (C_W), is sent to all secure devices just before the first key (C_W) is needed to decrypt the source signal.